

Privacy im Web 3.0: Leben im Glashaus?

Die digitale Welt bietet uns viel Komfort. Dabei geben wir aber viel von uns preis. Privatsphäre, früher so selbstverständlich wie heute die omnipräsente Vernetzung, geht in aller Stille flöten. Sie wird damit zunehmend zum knappen Gut.

Jeder kennt es: Man will sich auf einer Website registrieren. Das Passwort soll sicher und einzigartig sein, soll aber nirgends abgespeichert werden. Da ist es praktisch, wenn für die verschiedenen Websites stattdessen ein Social Login wie «Facebook Login» oder «Google Sign-In» genutzt werden kann. Dieses zentrale Login lässt sich zudem absichern, etwa durch eine Zwei-Faktor-Authentisierung oder risiko-basierte Sicherheitsmassnahmen bei ungewöhnlichem Nutzerverhalten.

Alles hat seinen Preis

Die Nutzung des Social Login ist für den Benutzer an sich kostenlos, doch bezahlt er mit seinen Profil- und Nutzungsdaten. An diesen Daten sind auch die Anbieter der Websites interessiert, die der Nutzer mittels Social Login nutzt. Zwar kann er die Weitergabe von Daten wie Profilbild, Alter und Freundesliste an Website-Anbieter mittlerweile steuern. Die Sammlung von Nutzungsdaten ist jedoch umfassend möglich. Diese geschieht teilweise auch im Sinne des Endkunden, etwa wenn sie hilft, mit Behaviour Analytics ungewöhnliches Verhalten zu erkennen und dadurch den missbräuchlichen Zugriff auf einen Account zu verhindern.

Security und Privacy sind auch beim Mobile Payment ein Thema. Neben dem Komfort des Bezahlens mit dem

Handy oder Peer-to-Peer-Überweisungen in Echtzeit kann man dabei von Sicherheitsfeatures wie dem Fingerabdrucksensor zur Zahlungsfreigabe profitieren, oder es werden alte Sicherheitsprobleme gelöst: So lassen sich Kreditkartendaten bei Apple Pay nicht mehr wie bei klassischen Magnetstreifenkarten kopieren und klonen. Dafür ist oft nicht klar: Wer hat nun genau Zugriff auf welche Daten? Werden diese nur für die Zahlungsvorgänge genutzt oder etwa auch für Profilbildung und Marketing oder die Forschung?

Fitnesstracker – seinen Daten hinterherrennen?

Auch das kleine Helferlein am Handgelenk erfasst Daten, misst Bewegung und Position, Herzfrequenz und sportliche Leistungen. Das hilft uns beim Erreichen der gesetzten Ziele. Werden über Apps weitere Details wie Schlaf oder Ernährung eingepflegt, mausert sich das Gerät bald zum unverzichtbaren Personal Trainer. Aufgrund der Korrelation von Daten bietet es aber auch jedem, der Zugriff auf die Daten hat, ein sehr umfassendes Bild des Endnutzers.

Der Endnutzer sollte sich also immer fragen, wem er seine Daten anvertraut, wem diese gehören, wie sie geschützt werden müssen und wer sie nutzen und korrelieren darf. Es gilt, sich selbst zu informieren und Verantwortung zu übernehmen, insbesondere in dynamischen Bereichen, in denen die Gesetzgeber nicht Schritt halten können.

Diese sind jedoch nicht untätig. Ab Mai 2018 gilt EU-weit die EU-Datenschutz-Grundverordnung (EU-DSGVO), die Endnutzern wie auch Unternehmen klarere Rechte und Pflichten zugesteht. Die Schweiz wird sich bei der aktuellen Revision des Datenschutzgesetzes wohl zugunsten der Kompatibilität daran anlehnen.

Security bedeutet nicht automatisch Privacy

Unternehmen sollten frühzeitig abschätzen, welche Möglichkeiten und Risiken daraus für sie entstehen. Die Frage, auf welche Technologien sie setzen, in welche Abhängigkeiten sie sich begeben, welche regulatorischen Auflagen sie zu beachten haben und welche Reputationsrisiken sie dabei eingehen, stellt sich ihnen ohnehin. Sie können dem Endkunden entgegenkommen, indem sie ihre Leistungen und Qualitätslevels auch hinsichtlich Privacy klar deklarieren. Insbesondere Schweizer Unternehmen können dabei neben der Swissness, der Qualität und der Sicherheit auch mit Privacy werben. Denn was bringt dem Kunden eine sichere Lösung, wenn seine Privatsphäre nicht mehr geschützt ist und er als Konsument im Glashaus präsentiert wird?



DER AUTOR



Thomas Zweifel
Principal IT
Consultant,
Adnovum



Bild: Fotolia